



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,442	12/06/2001	Jun Kim	0630-1373P	6382
2292	7590	08/24/2007		
BIRCH STEWART KOLASCH & BIRCH			EXAMINER	
PO BOX 747			BARTLEY, KENNETH	
FALLS CHURCH, VA 22040-0747				
			ART UNIT	PAPER NUMBER
			3693	
			NOTIFICATION DATE	DELIVERY MODE
			08/24/2007	ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

<b>Office Action Summary</b>	<b>Application No.</b> 10/003,442	<b>Applicant(s)</b> KIM, JUN	
	<b>Examiner</b> Kenneth L. Bartley	<b>Art Unit</b> 3693	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 16 May 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1 and 4-14 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. Receipt of Applicant's amendment and response filed on May 16, 2007 is acknowledged.

#### ***Response to Amendment***

2. Claims 1 and 4 are currently amended. Claims 2-3 have been cancelled. Claims 5-14 are new. Claims 1 and 4-14 are provided to be examined upon their merits.
3. The Examiner thanks the Applicant for response on priority and including it in the specification.
4. The Examiner thanks the Applicant for making the minor corrections to the specification.

#### ***Response to Arguments***

5. Applicant's arguments with respect to claims 1-9 have been considered but are moot in view of the new ground(s) of rejection.
6. Regarding Applicants arguments:
  - a. Applicant argues on page 10, 3<sup>rd</sup> paragraph:  
"In light of the foregoing amendments, Applicant respectfully submits that this rejection has been obviated and/or rendered moot. While not conceding to the Examiner's rejection, but merely to expedite prosecution, as the Examiner will note, independent claim 1 has been amended to incorporate the subject matter of claims 2 and 3. In particular, independent claim 1 has been amended to recite "changing the secret number to a new secret number after the transmitted encoded secret number has been determined to be identical to a previously registered secret number in the system, the step of changing the secret number to the new secret number including: encoding and transmitting the new secret

Art Unit: 3693

number to the system, and registering the new secret number in the system." Applicant respectfully submits that the above combination of steps as set forth in amended independent claim 1 is not disclosed or suggested by the references relied on by the Examiner."

**The Examiner respectively notes the amended changes and provides new grounds of rejection below.**

b. The Applicant points out that Clark fails to teach the step of changing a secret number to a new secret number in the last paragraph of page 10 and top of page 11:

"The Examiner has correctly acknowledged that Clark fails to teach changing the user's secret number. Although Clark discloses transmitting the encrypted secret number, the encrypted secret number is the current secret number. Clark nowhere discloses encrypting and then transmitting a new secret number, not to mention the fact that no new secret number is disclosed in Clark. Therefore, Clark fails to teach "the step of changing the secret number to the new secret number including: encoding and transmitting the new secret number to the system" as recited in amended claim 1."

Regarding Konheim, the Applicant continues on page 11, middle paragraph:

"Although Konheim discloses that the secret number may be arbitrarily choosable and alterable, Konheim fails to teach changing the secret number by encoding and transmitting the new secret number to the system as recited in amended claim 1. For example, as disclosed in the Background section of the instant application, although the secret number is alterable, the user may have to go to the bank in person to change it. Since Konheim simply discloses that the secret number is alterable without teaching how to change it, Konheim also fails to teach "the step of changing the secret number to the new secret number including: encoding and transmitting the new secret number to the system" as recited in amended claim 1."

**The Examiner provides new rejection below based on amended claims.**

c. In summary, the Applicant requests withdrawal of the rejection on page 11, 3<sup>rd</sup> paragraph:

Accordingly, the combination of Clark and Konheim fails to teach or suggest the limitations of amended independent claim 1. Therefore, Applicant respectfully submits that amended independent claim 1 and its dependent claims (at least due to their dependency) clearly define over the teachings of Clark and Konheim. Accordingly, reconsideration and withdrawal of the rejection under 35 U.S.C. § 103 are respectfully requested.

**The Examiner provides new grounds of rejection.**

**7. New grounds of rejection are presented below and have been modified to include consideration of the amended claims.**

***Claim Objections***

8. Claim 9 is objected to because of the following informalities: "access to the baking system..." should be "access to the banking system...". Appropriate correction is required.

***Claim Rejections - 35 USC § 112***

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 9-14 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

11. Claim 9 states "...a user's side remote to a banking system...". It is unclear what this means. For purposes of the examination, the Examiner interprets the portable card interface device to be attached to a user's computer. Claims 10-14 are rejected because they depend from claim 9.

***Claim Rejections - 35 USC § 103***

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 3693

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

13. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148

USPQ 459 (1966), that are applied for establishing a background for determining

obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

14. Claims 1, 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable

over U.S. Patent No. 5,517,569 to Clark in view of U.S. Patent 5,878,337 to Joao et al.

Regarding claims 1 and 5:

A home banking method comprising:

**Clark discloses:**

**A PC that can be used for home banking (col. 3, lines 61-57 and Fig. 1).**

reading and encoding coded information on a card;

**Smart and magnetic strip readers (col. 4, lines 42-52) for cards that contain encoded information (col. 10, lines 57-60). Therefore, information is able to be read and encoded to a card.**

transmitting the encoded information to a system connected to a remote computer network;

**"...a technique for transmitting encrypted data to a host computer from a remote personal computer." (col. 1, lines 7-10).**

inputting a secret number after receiving an indication that access to the system through the remote computer network has been allowed;

**"... a keypad which permits the user to directly enter confidential data (e.g. PIN) into the encryption module." (col. 2, lines 31-33) The system indicates, via a prompt, to the user to enter confidential information (col. 7, lines 16-20 and Fig. 8).**

encoding the secret number and transmitting the encoded secret number to the system;

Art Unit: 3693

**“The encryption module thereafter encrypts the confidential data and transmits the encrypted data to the PC, whereupon the encrypted data may be transmitted to the host computer via modem.” (col. 2, lines 33-36).**

changing the secret number to a new secret number after the transmitted encoded secret number has been determined to be identical to a previously registered secret number in the system, the step of changing the secret number to the new secret number including:

**(see below)**

encoding and transmitting the new secret number to the system, and

**Use of an encryption module to transmit PIN information...**

**“In accordance with this first embodiment, the encryption module comprises a keypad which permits the user to directly enter confidential data (e.g. PIN) into the encryption module.” (col. 2, lines 23-32)**

registering the new secret number in the system;

**(see below)**

requesting a user's home banking service transaction;

**User can “... select one or more banking options...for example a funds transfer operation...” (col. 6, lines 20-25)**

displaying a result of the user's home banking service transaction;

**Windows capability for performing banking operations (col. 5, lines 4-7 and Fig. 4), which allows results to be displayed.**

confirming the result of the user's home banking service transaction; and

**“Once host 102 has confirmed the transaction (col. 7, lines 49-53 and Fig. 8, Step 814)...”**

writing the result of the user's home banking service transaction on the card as encoded information.

**“The user may then be prompted to enter the smart card into a smart card reader/writer module... to effect the electronic update of the data resident on the smart card.” (col. 8, lines 11-15)**

**While Clark, in the business of bank transactions, provides for encryption using a PIN or secret number for a home banking system, he is silent on changing a user's secret number.**

**Joao et al., in the same business of bank transactions, teaches:**

**“With regards to automated teller machine accounts, it is also possible to specify and programmably change personal identification numbers and/or any other access code(s) and provide**

**for various personal identification numbers and/or access codes for different locations, different automated teller machines, different days, different times and/or different transaction amounts.” (col. 42, lines 56-62). It would be inherent that the PIN would be registered in a banking system for an ATM card. It is also inherent that in order to change a PIN, use of a PIN already registered in the system would be required.**

**Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to provide for changing secret numbers to new secret numbers at home, motivated by Joao et al., and that doing this would enhance security for a home banking system.**

Regarding claim 6:

The home banking method of claim 5, wherein the computer resides at the user's home.

**It is inherent that a home banking method would have a computer at a user's home.**

15. Claim 4 and 7-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over the reference as combined in section (14) above in further view of Official notice.

Regarding claim 4:

The home banking method of claim 1, wherein the step of changing the secret number to the new secret number further includes: confirming change to the new secret number by the user.

**While the references as combined in section (14) above provide for changing a secret number, they do not disclose changing the secret number and confirming the new secret number during the changing process. However, the Examiner takes Official Notice that confirming changes in secret numbers, PIN's, and passwords is old and well known. Therefore, it would have been obvious to one skilled in the art at the time of invention to require confirmation of a secret number, and that doing this would verify to the user that the system has registered the proper secret number, and that the user will then be able to access their account in the future.**

Regarding claim 7:

The home banking method of claim 5, wherein the step of encoding and transmitting the new secret number to the system includes:

**Clark discloses:**

**A PC that can be used for home banking (col. 3, lines 61-57 and Fig. 1)**



Art Unit: 3693

encoding the new secret number by a portable card interface device plugged into the computer; and

**Smart and magnetic strip readers (col. 4, lines 42-52) for cards that contain encoded information (col. 10, lines 57-60).**

**Such readers can be included with the encryption module and Fig. 2, ref. 214)...**

**"In accordance with the further aspect of the invention, the encryption module may be equipped with various peripheral devices useful in entering data and information, for example magnetic head card readers, "smart card" or integrated circuit card (ICC) readers, bar code readers, voice recognition devices, scanners, and the like." (col. 2, lines 56-62)**

**"... a keypad which permits the user to directly enter confidential data (e.g. PIN) into the encryption module." (col. 2, lines 31-33) The system indicates, via a prompt, to the user to enter confidential information (col. 7, lines 16-20 and Fig. 8).**

transmitting the new secret number from the computer to the system.

**"...a technique for transmitting encrypted data to a host computer from a remote personal computer." (col. 1, lines 7-10).**

**While the above references disclose connecting a portable card interface device to a computer, they do not disclose having the device "plugged" into the computer. However, the Examiner takes Official Notice plugging devices into computers is old and well known. Therefore, it would have been obvious to one skilled in the art at the time of invention to connect a card reader to a computer by plugging it in and that this would enhance the portability of the device.**

Regarding claim 8:

The home banking method of claim 7, wherein the step of writing the result of the user's home banking service transaction on the card includes:

receiving the result of the user's home banking service transaction from the system by the computer;

**Clark discloses:**

**A PC that can be used for home banking (col. 3, lines 61-57 and Fig. 1). The home banking system would allow for receiving banking service transaction information. Also, Fig. 1.**

encoding the result of the user's home banking service transaction by the portable card interface device;

Art Unit: 3693

**"In accordance with the further aspect of the invention, the encryption module may be equipped with various peripheral devices useful in entering data and information, for example... "smart card" or integrated circuit card (ICC) readers..." (col. 2, lines 56-61)**

writing the encoded result of the user's home banking service transaction on the card by the portable card interface device.

**The user may then be prompted to enter the smart card into a smart card reader/writer module (not shown) affiliated with either PC 110 or module 214 to effect the electronic update of the data resident on the smart card. (col. 8, lines 11-15)**

Regarding claims 9 and 10:

A home banking method comprising:

**Clark discloses:**

**A PC that can be used for home banking (col. 3, lines 61-57 and Fig. 1)**

plugging a portable card interface device into a computer at a user's side remote to a banking system;

**A portable card interface device into a computer...**

**"In the illustrated embodiment, module 214 suitably comprises a module connector 212 configured to permit easy installation of module 214. More particularly, a distal end 216 of connection 210 is normally plugged into a mating connector (not shown) on box 204 during normal operation of the PC." (col. 4, lines 16-25)**

**Access to a banking system...**

**"When an individual desires to effect a financial transaction, for example to order merchandise and pay for the merchandise with a credit card, the user constructs a data link between his PC and the host computer via the PC's modem." (col. 1, lines 25-29) Also, Fig. 1, ref. 106**

**While the above reference discloses connecting a portable card interface device to a computer and plugging into a mating connector, it does not disclose other connections being "plugged" into the computer. However, the Examiner takes Official Notice plugging devices into computers is old and well known. Therefore, it would have been obvious to one skilled in the art at the time of invention to connect a card reader to a computer by plugging it in and that this would enhance the portability of the device.**

reading and encoding coded information on a card by the portable card interface device;

**Smart and magnetic strip readers (col. 4, lines 42-52) for cards that contain encoded information (col. 10, lines 57-60).**

Art Unit: 3693

**Such readers can be included with the encryption module and Fig. 2, ref. 214)...**

**"In accordance with the further aspect of the invention, the encryption module may be equipped with various peripheral devices useful in entering data and information, for example magnetic head card readers, "smart card" or integrated circuit card (ICC) readers, bar code readers, voice recognition devices, scanners, and the like." (col. 2, lines 56-62)**

transmitting the encoded information from the computer to the banking system via a remote computer network;

**"The <encryption> module thereafter encrypts the confidential data and transmits the encrypted data to the PC, whereupon the encrypted data may be transmitted to the host computer via modem." (col. 2, lines 33-36).**

inputting a secret number after receiving an indication that access to the banking system has been allowed;

**"... a keypad which permits the user to directly enter confidential data (e.g. PIN) into the encryption module." (col. 2, lines 31-33) The system indicates, via a prompt, to the user to enter confidential information (col. 7, lines 16-20 and Fig. 8). Also, Fig. 8, ref. 804 indicates that the information is for a bank.**

encoding the secret number by the portable card interface device and transmitting the encoded secret number from the computer to the banking system; and

**"The encryption module thereafter encrypts the confidential data and transmits the encrypted data to the PC, whereupon the encrypted data may be transmitted to the host computer via modem." (col. 2, lines 33-36). Fig. 1, ref. 106, provides connection to a banking system.**

changing the secret number to a new secret number after the transmitted encoded secret number has been determined to be identical to a previously registered secret number in the banking system, the step of changing the secret number to the new secret number including: encoding and transmitting the new secret number to the banking system, and registering the new secret number in the banking system.

**While Clark, in the business of bank transactions, provides for encryption using a PIN or secret number for a home banking system, he is silent on changing a user's secret number.**

**Joao et al., in the same business of bank transactions, teaches:**

**"With regards to automated teller machine accounts, it is also possible to specify and programmably change personal identification numbers and/or any other access code(s) and provide for various personal identification numbers and/or access codes for different locations, different automated teller machines, different days, different times and/or different transaction amounts." (col. 42,**

Art Unit: 3693

**lines 56-62). It would be inherent that the PIN would be registered in a banking system for an ATM card. It is also inherent that in order to change a PIN, use of a PIN already registered in the system would be required.**

**Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to provide for changing secret numbers to new secret numbers at home by computer, motivated by Joao et al., and that doing this would enhance security of a home banking system.**

Regarding claim 11:

The home banking method of claim 9, wherein the step of encoding and transmitting the new secret number to the banking system includes:

encoding the new secret number by the portable card interface device, and

**Use of an encryption module to transmit PIN information...**

**"In accordance with this first embodiment, the encryption module comprises a keypad which permits the user to directly enter confidential data (e.g. PIN) into the encryption module." (col. 2, lines 23-32)**

transmitting the new secret number from the computer to the banking system.

**"The encryption module thereafter encrypts the confidential data and transmits the encrypted data to the PC, whereupon the encrypted data may be transmitted to the host computer via modem." (col. 2, lines 33-36)**

Regarding claim 12:

The home banking method of claim 9, further comprising:

requesting a user's home banking service transaction;

**Clark discloses:**

**"...the user may select banking operation 406 corresponding to icon 506..." (col. 5, lines 7-10) and Fig. 4.**

displaying a result of the user's home banking service transaction;

**"...if the user desires to inquire as to an account balance and/or status (Step 604), the system may suitably be configured to prompt the user to select a particular account subject to inquiry (Steps 612), whereupon the system suitably returns to Step 712 (see FIG. 7)." (col. 7, lines 54-59)**

confirming the result of the user's home banking service transaction; and

**Using a printer to confirm the transaction...**

**"In addition, the system may be configured to require a functioning printer as a prerequisite to effecting the foregoing smart card updating function, as desired." (col. 8, lines 15-18)**

Art Unit: 3693

writing the result of the user's home banking service transaction on the card as encoded information.

**The user may then be prompted to enter the smart card into a smart card reader/writer module (not shown) affiliated with either PC 110 or module 214 to effect the electronic update of the data resident on the smart card. (col. 8, lines 11-15)**

Regarding claim 13:

The home banking method of claim 12, wherein the step of writing the result of the user's home banking service transaction on the card includes:

receiving the result of the user's home banking service transaction from the banking system by the computer;

**Clark discloses:**

**"...integrated circuit cards (ICC), also known as smart cards, typically comprise a microprocessor embedded within the card, as well as an electronic mechanism for permitting data transfer to and from the card. That being the case, account information and, indeed, funds may be electronically "added" to or "subtracted" from the card by making appropriate modification to the data resident on the card." (col. 7, lines 64-67 and col. 8, lines 1-5)**

encoding the result of the user's home banking service transaction by the portable card interface device;

**"In accordance with the further aspect of the invention, the encryption module may be equipped with various peripheral devices useful in entering data and information, for example... "smart card" or integrated circuit card (ICC) readers..." (col. 2, lines 56-61)**

Regarding claim 14:

The home banking method of claim 9, wherein the computer resides at the user's home.

**It is inherent that a home banking method would have a computer at a user's home.**

***Conclusion***

16. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

Art Unit: 3693

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

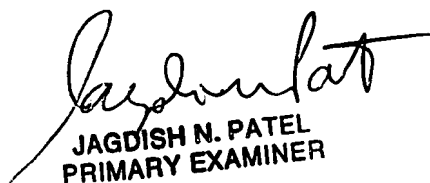
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kenneth L. Bartley whose telephone number is (571) 272-5230. The examiner can normally be reached on Monday through Friday, 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jagdish Patel can be reached on (571) 272-6748. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 3693

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



JAGDISH N. PATEL  
PRIMARY EXAMINER